REMARKS

Claims 1 and 4-14 were examined by the Office, and in the Office Action of April 18, 2008 all claims are rejected. With this response claims 1, 4, 6-10 and 12 are amended to place the claims in better form. All amendments are fully supported by the specification as originally filed.

Applicant respectfully requests reconsideration and withdrawal of the rejections in view of the following discussion.

Claim Rejections Under § 103

In section 3, on page 2 of the Office Action, claims 1, 4-14 are rejected under 35 U.S.C. § 103(a) as unpatentable over Grohoski (U.S. Appl. Publ. No. 2004/0225885) in view of Srinivasan et al. (U.S. Appl. Publ. No. 2004/0158742). Applicant respectfully submits that the cited references, alone or in combination, fail to disclose or suggest all of the limitations recited in claim 1. Applicant respectfully submits that the cited references at least fail to disclose or suggest that the configuration register is configured to receive mode setting instructions from a protected application.

On page 3 of the Office Action, the Office acknowledges that Grohoski fails to disclose a configuration register configured to receive mode setting instructions from a protected application, and relies upon Srinivasan for this teaching. However, Srinivasan also fails to disclose or suggest that the configuration register is configured to receive mode setting instructions from a protected application, as recited in claim 1. In contrast to claim 1, Srinivasan only discloses that in a step (216) the trusted server optionally verifies that the secure processor (110) is authorized to receive application software from the trusted server. See Srinivasan paragraph [0105]. However, Srinivasan further states that the CPU operating in secure mode receives the application software or other additional instructions from the trusted server. See Srinivasan paragraph [0107]. If the CPU is already operating in a secure mode before the application software is received from the trusted server, then the application software cannot be considered to be a protected application that provides mode setting instructions to a configuration register, as recited in claim 1.

In fact, Srinivasan defines "application software' as a set of instructions or parameters capable of being executed or interpreted by a processor. See Srinivasan paragraph [0031]. Srinivasan makes no mentioned that the application software is a protected application as mentioned in claim 1. Therefore, the section relied upon by the Office do not disclose a configuration register configured to receive mode setting instructions from a protected application, as recited in claim 1. Instead, these sections only disclose that the application software places parameters for a request for services in a set of selected registers, or performs an uncached read to a register. See Srinivasan paragraphs [0121] & [0127]. Even if the application software are considered to be a protected application, which applicant does not admit, the functions performed by the application software in Srinivasan do not correspond to providing mode setting instructions, as recited in claim 1.

Furthermore, while Srinivasan defines "secure code" and "secure boot loader code" to be interpretable or executable by the secure processor, and known to the secure processor to be trustable, the secure code and secure boot loader code do not provide mode setting instructions to a configuration register. Claim 1 recites that the configuration register is configured to receive mode setting instructions from a protected application, however even if the secure code and secure boot loader code are considered to correspond to the protected application Srinivasan does not disclose a configuration register configured to receive mode setting instructions from the secure code or the secure boot loader code. Instead, after power on of the secure processor (110) a reset signal (A170) is asserted that indicates that the secure processor (110) has been reset. See Srinivasan paragraph [0088]. As a result, the secure mode active signal (A160) is asserted and the CPU transfers execution control to the secure boot code (A115). The secure mode active signal (A160) indicates to the non-volatile memory that the CPU is allowed to access the secure boot code, execute its instruction, and read and write data using the security information (113). See Srinivasan paragraph [0089]. However, Srinivasan does not disclose or suggest that a configuration register receives mode setting instructions from a protected application, instead it appears that the reset signal (A170) is responsible for setting the secure processor (110). Therefore, for at least these reasons claim 1 is not disclosed or suggested by the cited references.

Independent claim 12 is amended in a manner similar to claim 1, and contains limitations similar to claim 1. Therefore, for at least the reasons discussed above in relation to claim 1, claim 12 is not disclosed or suggested by the cited references.

The dependent claims depending from the above mentioned independent claims are not disclosed or suggested by the cited references at least in view of their dependencies.

Conclusion

It is therefore respectfully submitted that the present application is in condition for allowance and such action is earnestly solicited. The undersigned authorizes the Commissioner to charge any fees required to submit this response to Deposit Account No. 23-0442.

Respectfully submitted,

Dated: 16 July 2008

s/Keith R. Obert/
Keith R. Obert
Attorney for Applicant
Registration No. 58,051

WARE, FRESSOLA, VAN DER SLUYS
& ADOLPHSON LLP
Bradford Green, Building Five
755 Main Street, P.O. Box 224
Monroe, CT 06468
Telephone: (203) 261-1234
Facsimile: (203) 261-5676
USPTO Customer No. 004955